Department of Homeland Security Daily Open Source Infrastructure Report for 28 April 2006

Current Nationwide Threat Level is
ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS
For info click here
http://www.dhs.gov/

Daily Highlights

- Newsday reports the Long Island Rail Road said Wednesday, April 26, that it has lost personal information −− names, addresses, Social Security numbers, and salary figures −− of virtually everyone who has ever worked for the agency. (See item 8)

- The Associated Press reports police confronted a man at a Cleveland Hopkins International Airport ticket counter on Thursday, April 27; shots were fired as they struggled, critically wounding a patrolman and killing the man. (See item 16)

- The Associated Press reports a new computer simulation from Department of Infectious Disease Epidemiology at Imperial College in London shows that if pandemic influenza arrives in the U.S. next year, the few weapons the country has to keep it from spreading will do little good. (See item 30)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *April 27, Christian Science Monitor* — **With oil at $70 a barrel, firms try coal, shale, even turkeys.** At more than $70 a barrel, the price of oil is signaling for some people an opportunity to move the United States beyond conventional oil. In Carthage, MO, a company is turning the

inedible parts of Butterball turkeys into up to 350 barrels of biodiesel per day. In Gilberton, PA, businessman John Rich is planning to convert huge piles of low−quality coal into diesel. The state has promised to buy the production of 5,000 barrels per day, once it starts. In Utah and Colorado, four companies are preparing environmental assessments to show the feasibility of producing oil from shale. With gas now becoming as pricey as a gallon of milk in some places, the economics of energy production is changing. Processes that didn't make any sense years ago are now being pulled out of filing cabinets. From the tundra of Alaska to the depths of the Gulf of Mexico, energy dreamers are trying to tap into new frontiers. The potential reserves in some cases are gigantic. The Bureau of Land Management has estimated the potential U.S. recoverable oil shale reserves at 800 billion barrels of oil, three times the proven oil reserves of Saudi Arabia.
Source: http://www.csmonitor.com/2006/0427/p02s02−usec.html

2. *April 26, Associated Press* — **Duke Energy to build natural gas pipeline, expand transmission system.** Duke Energy Corp. said that it plans to build a natural gas pipeline in two Cape Cod, MA, towns to expand its Algonquin gas transmission system. The company said the 3.5−mile, 18−inch diameter pipeline will provide KeySpan Corp. with 38,000 dekatherms per day of natural gas under a 15−year agreement. The pipeline will be constructed in Sandwich and Bourne, MA. The project was filed last week with the Federal Energy Regulatory Commission, and Duke said it plans to seek federal, state and local permits this year and early next year. Duke said it expects construction to begin next spring, with service to begin in the following November.
Source: http://biz.yahoo.com/ap/060426/duke_energy_pipeline.html?.v= 1

3. *April 26, Associated Press* — **Adequate summer electricity supplies seen for Northeast.** Power grid managers say electricity supplies in the Northeast this summer will be adequate to handle the region's power needs, even if there's a long heat wave. But with extreme temperatures or grid problems, the Boston area and southwestern Connecticut are spots where emergency measures might have to be taken to prevent outages. A report released Wednesday, April 26, from the Northeast Power Coordinating Council said steps could include interrupting power to certain major electricity customers with interruptible supply contracts. The council says two other potential problem spots facing a lesser risk are New York City and Long Island. Electricity supplies are more robust in other areas of the Northeast.
Northeast Power Coordinating Council report: http://www.npcc.org/news.cfm
Source: http://www.capitalnews9.com/content/headlines/?ArID=177054&S ecID=33

4. *April 26, Associated Press* — **Man shocked inside Duke substation.** A 25−year−old man was hospitalized after he was shocked after he entered a Duke Energy substation near Kings Mountain, NC. Police are not sure why Frankie James Dobbins entered the substation. Dobbins was discovered after Duke Energy sent a repair technician to the scene after the power went out. Duke Energy's substations have six−foot high fences with locked gates and signs indicating the potential dangers, company spokesperson Marylyn Lineberger said.
Source: http://www.news14charlotte.com/content/local_news/?ArID=1184 61&SecID=2

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

5. *April 27, Aviation Now* — **Navy satellite services consolidated contract under trial.** The Defense Information Systems Agency (DISA) and the Navy are working to consolidate the Navy's 16 worldwide satellite communications requirements under one task order via the Defense Information Systems Network Satellite Transmission Services−Global (DSTS−G) program. DISA has issued a solicitation under DSTS−G for a new consolidated contract, the congressional Government Accountability Office reported Monday, April 17. The experiment comes as the Department of Defense is re−examining how it procures commercial satellite services due to criticism of lengthy, inflexible and costly commercial satellite services acquisition.
Source: http://www.aviationnow.com/avnow/news/channel_netdefense_story.jsp?id=news/SEN04276.xml

6. *April 26, Government Accountability Office* — **GAO−06−446: Electronic Warfare: Option of Upgrading Additional EA−6Bs Could Reduce Risk in Development of EA−18G (Report).** The EA−6B has conducted airborne electronic attack for all services since 1996. In 2002, the Department of Defense (DoD) completed an analysis of alternatives for the EA− 6B that concluded the inventory would be insufficient to meet the DoD’s needs beyond 2009. Since then, the services have embarked on separate acquisition efforts to develop airborne electronic attack assets. In 2003, the Navy started development of the EA−18G aircraft to replace the EA−6B. This report assesses if (1) DoD’s 2002 conclusion that the EA−6B inventory would be insufficient beyond 2009 remains valid for assessing the Navy’s future needs, and (2) the acquisition approach used to develop the EA−18G is knowledgebased and might mitigate future risks. The Government Accountability Office (GAO) recommends that DoD determine how many EA−6Bs with upgraded electronic suites are needed to deal with the existing and near−term capability gap, and consider procuring them. If DoD does this, it should cancel plans to end the electronic suite production line after 2006. If DoD outfits more EA−6Bs with upgraded electronic suites, it should restructure its EA− 18G low−rate initial production plans so that procurement occurs after the aircraft demonstrates it is fully functional. DoD partially concurred with our recommendations.
Highlights: http://www.gao.gov/highlights/d06446high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−446

[Return to top]

Banking and Finance Sector

7. *April 27, Websense Security Labs* — **Phishing Alert: Columbus Bank and Trust.** Websense Security Labs has received reports of a new phishing attack that targets customers of Georgia−based Columbus Bank and Trust. Users receive a spoofed e−mail message, which claims that due to multiple login failures, their account could be compromised and now has

limited access. This message provides a link to a phishing Website, which prompts users to enter account information to resolve the issue.
Source: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =475

8. *April 27, Newsday* — **LIRR loses records.** The Long Island Rail Road (LIRR) said Wednesday, April 26, that it has lost personal information −− names, addresses, Social Security numbers, and salary figures −− of virtually everyone who has ever worked for the agency. Iron Mountain, Inc., a Boston company employed by the railroad to warehouse and secure information at an undisclosed storage site in the metropolitan area, discovered the loss on April 6, LIRR and Iron Mountain officials said. During a routine delivery between LIRR headquarters in Jamaica, Queens, and the storage site, an Iron Mountain driver noticed that at least one unmarked box containing "computerized back−up data tapes" was missing, LIRR officials said. Iron Mountain officials said they believed it was not likely the box was stolen. On Monday, the railroad mailed a two−page letter signed by LIRR president James Dermody to approximately 17,000 current and former employees notifying them about the lost information. The LIRR has about 6,000 current employees. Nevertheless, the LIRR has agreed to provide anyone at risk with a free one−year enrollment with a credit check and identity theft monitoring service. The railroad has also set up a Website and hotline, 888−324−8488, for employees with questions about the missing data.
Website: http://longislandrailroad.info/employeedatainfo/
Source: http://www.newsday.com/news/local/longisland/ny−lilirr0427,0 ,6367534.story?coll=ny−top−headlines

9. *April 26, Channel Register (UK)* — **Phishing goes international.** The number of phishing attacks targeting non−English speaking financial institutions is on the rise. Attacks targeting countries outside the English−speaking world now represents almost 40 percent of worldwide phishing targets, according to data processed by RSA Security's Anti−Fraud Command Center. RSA said it has shut down more than 10,000 phishing attacks hosted in 70 different countries. The primary phishing targets worldwide still remain English speaking countries such as the U.S. and the UK, followed by Australia and Canada. The U.S. alone accounts for approximately half of fraudulent e−mail attacks. Over the last six months or so there's been an upswing in attacks targeting European countries, including Spain, Germany, and Italy, as well as the Netherlands, Scandinavia, and France. E−mails are even being sent in local languages, such as Catalan, with fraudulent Websites designed to circumvent protection mechanisms such as scratch cards with random access codes, or lists of one time transaction access numbers held by the bank's customers. RSA says the trend is down to a combination of factors including an increase in the number of online banking users in Europe and Asia Pacific, and banks offering increased functionality as part of online services.
Source: http://www.channelregister.co.uk/2006/04/26/international_ph ishing_survey/

10. *April 26, Marines.com* — **Credit reports help Marines safeguard identity.** Headquarters Marine Corps officials recently announced that 207,750 enlisted Marines, who served in the Marine Corps between 2001 and 2005, are at risk of identity theft due to the loss of personal information. The lost information included name, social security number, marital status, and enlistment contract information. Although the information was lost aboard a military installation, it is still considered to be a very serious risk to all personnel who were affected, according to Staff Sgt. Ryan M. Chilson, information assurance manager here. There is no

evidence the information has been compromised and Naval Postgraduate School officials are currently conducting a detailed investigation to determine the facts surrounding the case, according to Marine Administration message 143/06.
Source: http://www.usmc.mil/marinelink/mcn2000.nsf/main5/9F14BD861DD DBAEE8525715C002180B6?opendocument

11. *April 26, WJACTV 6 (PA)* — **Pennsylvania bank issues scam warning.** First National Bank (FNB) in Pennsylvania warns that some customers may be the victims of an e−mail scam. The statement on the bank's Website claims that someone sent e−mail to some customers stating that an FNB account had been disabled. The e−mail then asked recipients to click a link. That link took them to a site which looked like the FNB site, which prompted them for account numbers. Bank officials aren't sure how many people received the fraudulent e−mail or how many responded.
Source: http://www.wjactv.com/news/9016499/detail.html?rss=john&psp= news

12. *April 26, SC Magazine (UK)* — **New mobile virus warning.** Security experts warned mobile phone users that a new virus is charging them several dollars to send a premium rate text message. Speaking at Infosec Europe 2006, anti−virus company F−Secure found a proof−of−concept virus developed to steal money from mobile customers. "This virus gets your mobile phone to text a premium−rate number and then it sends an authority that can then charge you without your knowledge," said Richard Hales of F−Secure. Hales said the new virus was similar to the CommWarrior virus that propagated itself via multimedia messages and Bluetooth.
Source: http://www.scmagazine.com/uk/news/article/555740/new+mobile+ virus+warning/

13. *April 26, CNET News* — **Scammers steal details on 2,000 credit cards.** Scammers stole the credit card details of 2,000 MasterCard holders in a major security breach last week. Silicon.com was contacted by one customer of the Clydesdale Bank in the UK, who was told that her MasterCard details, along with those of 2,000 other people, were "in the hands of a [scammer]." The theft was detected and the card stopped before it could be used by the scammer. MasterCard said it took immediate action together with all the banks concerned as soon as the breach was discovered. MasterCard didn't say how the breach occurred, whether it was limited to the UK or which issuing banks were affected besides the Clydesdale.
Source: http://news.com.com/Fraudsters+steal+details+on+2%2C000+cred it+cards/2100−7349_3−6065267.html?tag=cd.top

14. *April 26, Reuters* — **Aetna says computer with member information stolen.** Health insurer Aetna Inc. on Wednesday, April 26, said a laptop computer containing personal information on about 38,000 of its members was stolen from an employee's car. The data includes names, addresses, and Social Security numbers, spokesperson Cynthia Michener said. No personal banking information or health claim data was on the laptop, she added. The members are employees of two companies that are Aetna customers, the company said in a statement. Michener said the two companies had asked that their names not be disclosed. According to the statement, there was no indication that data on the laptop had been compromised. The car was broken into while it was in an outdoor public parking lot, and the doors were locked, Michener said. Michener declined to say in which city or state the theft occurred. She said the company is working with law enforcement authorities.

Source: http://news.yahoo.com/s/nm/20060427/bs_nm/aetna_data_dc_1

[Return to top]

Transportation and Border Security Sector

15. *April 27, Government Accountability Office* — **GAO−06−588T: Gas Pipeline Safety: Preliminary Observations on the Implementation of the Integrity Management Program (Testimony).** About a dozen people are killed or injured in natural gas transmission pipeline incidents each year. In an effort to improve upon this safety record, the Pipeline Safety Improvement Act of 2002 requires that operators assess pipeline segments in about 20,000 miles of highly populated or frequented areas for safety risks, such as corrosion, welding defects, or incorrect operation. Half of these baseline assessments must be done by December 2007, and the remainder by December 2012. Operators must then repair or replace any defective pipelines, and reassess these pipeline segments for corrosion damage at least every 7 years. The Pipeline and Hazardous Materials Safety Administration (PHMSA) administers this program, called gas integrity management. This testimony is based on ongoing work for this Subcommittee and for other committees, as required by the 2002 act. The testimony provides preliminary results on the safety effects of (1) PHMSA's gas integrity management program and (2) the requirement that operators reassess their natural gas pipelines at least every seven years. It also discusses how PHMSA has acted to strengthen its enforcement program in response to recommendations the Government Accountability Office (GAO) made in 2004. GAO expects to issue two reports this fall that will address these and other topics.
Highlights: http://www.gao.gov/highlights/d06588thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−588T

16. *April 27, Associated Press* — **Man dies in Cleveland airport shooting; officer critically wounded.** Police confronted a man at a Cleveland Hopkins International Airport ticket counter Thursday, April 27, and shots were fired as they struggled, critically wounding a patrolman and killing the man, authorities said. The man grabbed one officer's gun and shot another officer twice in the chest, city Safety Director Martin Flask said. The shooting was in an area before security checkpoints. The airport remained open, said Fred Szabo, director of the airport. "We have several witnesses who saw it happen, a number of police officers, Transportation Security Administration employees and some passengers as well," Szabo said.
Source: http://www.cnn.com/2006/US/04/27/airport.shooting.ap/index.h tml

17. *April 27, Memphis Business Journal* — **Pinnacle Airlines profits down.** Pinnacle Airlines Corp., which is based in Memphis, TN, operates a regional airline under the name Northwest Airlink that provides airline capacity to Northwest Airlines Corp Pinnacle said net income for the first quarter was $13.3 million, or 61 cents per share, a 43 percent decrease compared with net income of $23.3 million, or $1.06 per share, in first quarter 2005. Management says a key goal for Pinnacle in the near future remains securing the company's existing business relationship with Northwest Airlines. n December 2005, Pinnacle reported that Northwest Airlines, which filed for Chapter 11 bankruptcy in September, had sent a request for proposal to Pinnacle and other airlines asking for proposals to operate a number of 76−seat regional jets comparable to the number of aircraft currently comprising Pinnacle's fleet. As part of its discussions with Northwest, Pinnacle hopes to resolve the issue of its outstanding security

deposits totaling $21.7 million related to aircraft subleases between Northwest and Pinnacle.
Source: http://biz.yahoo.com/bizj/060427/1278964.html?.v=1

18. *April 27, Associated Press* — **Delta, Aeromexico partner on maintenance.** Delta Air Lines Inc., which has cut maintenance jobs as part of its restructuring, is partnering with Aeromexico to market and perform repair work for customers worldwide. The United States' third−largest airline and the Mexican carrier said Wednesday, April 26, that the deal will allow Aeromexico to expand its airframe heavy maintenance capabilities and Atlanta−based Delta to expand its maintenance, repair and overhaul services business. The companies also said that Delta's technical operations division will become the exclusive maintenance provider for Aeromexico's fleet of CFM56−7 engines and 131−9B auxiliary power units, while Aeromexico will become the exclusive heavy maintenance provider for Delta's MD−88 fleet. In January, the company, which is operating under bankruptcy protection, said it would cut up to 1,000 maintenance jobs by April 1 as part of its previous announcement to cut up to 9,000 jobs companywide.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/04/26/AR2006042602091.html

[Return to top]

Postal and Shipping Sector

Nothing to report.

[Return to top]

Agriculture Sector

19. *April 27, American Phytopathological Society* — **First report of northern stem canker of soybean caused by Diaporthe phaseolorum var. caulivora in North Dakota.** In early September 2003, patches of soybean (Glycine max) plants in a field in Foster County, ND, had dead branches with reddish brown cankers at the nodes. Cultures were identified as Diaporthe phaseolorum var. caulivora. According to North Dakota State University's Department of Plant Pathology, this is the first report in North Dakota from samples collected in 2003. Stem canker has been reported in Europe, South America, and in most soybean regions of Canada and the United States. It has been widely recognized as an important soybean disease, but recently has been divided into northern stem canker and southern stem canker based on two causal agents. Northern stem canker was first reported in the late 1940s in Iowa, and by the 1950s, the disease had spread into the upper Midwest and Canada. Southern stem canker was reported in the south in 1973, and by 1984, had been detected in all southern states. Northern stem canker and southern stem canker are caused by Diaporthe phaseolorum var. caulivora and Diaporthe phaseolorum var. meridionalis, respectively. Additional information found at: http://www.plantpath.wisc.edu/soyhealth/pdf/stemcanker_06.pd f
Also see: http://www.soydiseases.uiuc.edu/index.cfm?category=diseases& disease=95
Source: http://www.apsnet.org/pd/searchnotes/2006/PD−90−0687A.asp

20. *April 26, U.S. Department of Agriculture* — **USDA amends tuberculosis regulations regarding re−accreditation test for captive cervids.** The U.S. Department of Agriculture’s

(USDA) Animal and Plant Health Inspection Service is amending the regulations regarding bovine tuberculosis in captive cervids in order to reduce testing costs for herd owners, lessen the potential for animal injury or death during testing, lower administrative costs for state and federal regulatory agencies and continue to protect American agriculture. Bovine tuberculosis is a contagious and infectious disease caused by Mycobacterium bovis. This final rule became effective Friday, April 21.
Source: http://www.aphis.usda.gov/newsroom/content/2006/04/tbtest_vs .shtml

21. *April 26, U.S. Department of Agriculture* — **USDA proposes amendments to import regulations on fruits and vegetables.** The U.S. Department of Agriculture's Animal and Plant Health Inspection Service (APHIS) Wednesday, April 26, announced a proposal to establish criteria within its regulations that would allow APHIS to approve or reject certain fruits and vegetables for importation into the United States and to acknowledge pest−free areas in foreign countries using a notice−based process. A series of public meetings on the proposed amendments will be held in Los Angeles, CA, Seattle, WA, and Miami, FL, the week of May 23 and in Washington, DC, on Tuesday, June 20. The proposed process for approving imports would apply only to commodities that can be safely imported subject to inspection, treatment and/or certification that the commodity is pest free in the country of origin. The importation of fruits and vegetables that require additional phytosanitary measures would continue to require specific prior rulemaking. APHIS will seek public comment on import requests by publishing notices in the Federal Register inviting comment on the findings of pest−risk analyses prior to authorizing any imports via follow−up notices.
Source: http://www.aphis.usda.gov/newsroom/content/2006/04/q56meet.s html

22. *April 23, Associated Press* — **Tests: Pigeons don't pose bird flu trouble.** Although pigeons are not immune to the bird flu virus, tests indicate: the birds pick it up only when they are exposed to very high doses; they do not always become infected under those conditions and are carriers only briefly. In one experiment conducted by the Department of Agriculture's Southeast Poultry Research Laboratory, researchers squirted into pigeons' mouths liquid drops that contained the highly pathogenic H5N1 virus. "We couldn't infect the pigeons," said the lab's director, David Swayne. In 2004, the lab did two more experiments. Seven became infected and one died. Five others did not become infected. "The experimental data is not very strong that pigeons are going to be spreading this virus around," Swayne said.
Agricultural Research Service: http://www.ars.usda.gov/main/
Source: http://abcnews.go.com/Health/wireStory?id=1880086&page=1

23. *April 19, World Organization for Animal Health* — **West Nile outbreak in Argentina reported.** Two outbreaks of West Nile fever have been reported in San Antonio de Areco, Buenos Aires province of Argentina. They have occurred in two breeding farms of pure−bred racehorses. The diagnosis was established on Wednesday, April 19, at the National Institute of Human Viral Diseases, by Dr. Julio I Maistegui. This disease has never been reported before in Argentina.
Source: http://www.oie.int/Messages/060425ARG.htm

[Return to top]

Food Sector

24. *April 27, USAgNet* — **South Korea to resume U.S. beef imports.** South Korea, the third−biggest buyer of U.S. beef in 2003, will resume imports from the U.S. after confirming a cow infected with mad−cow disease in Alabama was born before feed restrictions were imposed. The confirmation means inspection procedures that were suspended last month will be resumed.
Source: http://www.usagnet.com/story−national.cfm?Id=753&yr=2006

25. *April 27, USAgNet* — **Nineteen animals traced to latest bovine spongiform encephalopathy case in British Columbia.** The Canadian Food Inspection Agency will be testing 19 animals connected to a cow discovered with mad cow disease on a dairy farm in the Fraser Valley. George Luterbach, spokesperson for the agency, said Tuesday, April 25, the cattle may have eaten the same feed consumed by an animal infected with bovine spongiform encephalopathy.
Source: http://www.usagnet.com/story−national.cfm?Id=754&yr=2006

26. *April 27, BBC News (UK)* — **Chicken cull after bird flu find.** Some 35,000 chickens at a poultry farm in Norfolk, UK, are to be slaughtered after dead birds tested positive for a strain of bird flu. The government's chief veterinarian said it was likely to be the H7 strain, virulent among chickens but less of a threat to humans than the H5N1 variant. Last month a swan in Cellardyke, Fife, tested positive for H5N1 −− the only confirmed case in the UK so far. Dr. Debbie Reynolds said there was so far no evidence of the H5N1 strain in the chickens from the Norfolk farm.
Source: http://news.bbc.co.uk/2/hi/uk_news/4949026.stm

27. *April 26, Center for Infectious Disease Research & Policy (University of Minnesota)* — **Antibacterial bacteria may be used in ground beef.** Food stores may soon be able to offer ground beef and other meat products treated with a mixture of harmless bacteria that reportedly can reduce common pathogens by 99 percent or more. The mixture contains four strains of lactic acid bacteria, a class of organisms that has long been used in cultured dairy products such as yogurt and cheese. In a study reported last year in the Journal of Food Protection, the mixture, called Bovamine Meat Cultures, progressively reduced the levels of Escherichia coli O157:H7 and Salmonella in ground beef during several days of refrigerated storage. Last December the Food and Drug Administration (FDA) classified the product as "generally regarded as safe," clearing the way for commercial use.
Abstract (full text article available for purchase:
http://www.ingentaconnect.com/content/iafp/jfp/2005/00000068 /00000008/art00005
April 20 Texas Tech news release: http://www.texastech.edu/stories/0604−brashears.php
FDA letter regarding safety of lactic acid bacteria mixture:
http://www.cfsan.fda.gov/~rdb/opa−g171.html
Source: http://www.cidrap.umn.edu/cidrap/content/fs/food−disease/new s/april2606lacto.html

[Return to top]

Water Sector

28. *April 26, Baltimore Sun (MD)* — **MTBE found in Maryland wells.** Water from a well serving

about 40 homes in a Finksburg, MD, trailer park has tested positive for contamination from the gasoline additive MTBE, according to the Carroll County Health Department. Officials from the county and Maryland Department of the Environment are uncertain of the contaminant's source, said Brian Flynn, water quality supervisor for the Health Department. Preliminary tests at area gas stations and an auto−parts junkyard near Sullivan's Trailer Park along Old Westminster Pike yielded negative results, Flynn said.
Source: http://www.baltimoresun.com/news/local/carroll/bal−md.ca.mtb e26apr26,0,6280197.story?track=rss

[Return to top]

Public Health Sector

29. *April 27, Associated Press* — **Report says not enough info on flu masks.** If a worldwide flu epidemic strikes, face masks should be considered a defense of last resort since there's little evidence about whether the masks available to the average person or most health care workers can prevent influenza infection, the Institute of Medicine said Thursday, April 27. Certain filtering masks can protect wearers from specific respiratory diseases, such as tuberculosis. While N95 respirators haven't been tested to see how effectively they block flu virus specifically, they are designed to block small particles. But they must be individually fitted to users' faces so that air doesn't seep into the sides. Also, they come only in certain sizes, none for children. More expensive reusable masks do exist, but there is no good way to decontaminate and reuse surgical masks and standard disposable N95s, the panel concluded. Using a handkerchief or some other improvised mask are not likely to be as protective as even a surgical mask might be, but the panel hesitated to discourage them for people with no other options on the assumption that some protection might be better than none. Generally, the tighter the fabric weave, the better.
Source: http://www.latimes.com/news/nationworld/nation/wire/ats−ap_h ealth10apr27,1,4194693.story?coll=sns−ap−tophealth

30. *April 26, Associated Press* — **U.S. efforts might not slow pandemic flu.** If pandemic influenza hits in the next year, the few weapons the U.S. has to keep it from spreading will do little, a new computer model shows. A pandemic flu is likely to strike one in three people if nothing is done, according results published in the Thursday, April 27, edition of Nature. If the government acts fast enough and has enough antiviral medicine to use as preventive dosings −− which the U.S. does not −− that could drop to about 28 percent of the population getting sick, the study found. The computer simulation by Neil Ferguson of the Department of Infectious Disease Epidemiology at Imperial College in London is the second released this month and is more pessimistic than one led by Timothy Germann of Los Alamos National Laboratory, who said the flu could be less infectious and that efforts could slow it a bit. Closing schools to halt breeding grounds and the use of Tamiflu could reduce the disease's toll, Ferguson said. But efforts to stop flu from entering American borders −− usually on planes with sick passengers −− won't work, he said. At most, they can buy a couple of weeks of delay, he said.
Study: http://www.nature.com/nature/journal/vaop/ncurrent/full/natu re04795.html
Source: http://seattlepi.nwsource.com/health/1500AP_Preventing_Pande mic.html

31.

April 26, HealthDay News — **Vaccine could fight deadly Marburg virus.** A vaccine has proved effective in preventing hemorrhagic fever in monkeys after they were exposed to the deadly Marburg virus. Like the Ebola virus, Marburg causes internal bleeding at multiple sites in the body. Both viruses are considered to be potential bioterrorism threats. There are no drugs to fight infection with Marburg virus. The team of researchers from the U.S. Army Medical Research Institute of Infectious Diseases and the National Microbiology Laboratory at the Public Health Agency of Canada say they have created a vaccine by replacing a gene from a harmless virus with a gene encoding a surface protein on the Marburg virus. In their study, reported in the Thursday, April 27 issue of The Lancet, the researchers infected five monkeys with the Marburg virus. Three other monkeys acting as controls were infected with the virus but were given a vaccine without the Marburg protein. All five monkeys that received the Marburg protein vaccine survived for at least 80 days, while the controls died within 12 days. This study suggests the vaccine may be an effective post−infection treatment for the disease.
Marburg hemorrhagic fever information:
http://www.cdc.gov/ncidod/dvrd/spb/mnpages/dispages/marburg/ qa.htm
Lancet article summary (free registration required):
http://www.thelancet.com/journals/lancet/article/PIIS0140673 606685462/abstract?iseop=true
Source: http://www.forbes.com/forbeslife/health/feeds/hscout/2006/04 /26/hscout532340.html

[Return to top]

Government Sector

32. *April 27, Government Accountability Office* — **GAO−06−665T: Capitol Visitor Center: Update on Status of Project's Schedule and Cost as of April 27, 2006 (Testimony).** Since the Subcommittee’s March 15 Capitol Visitor Center (CVC) hearing, the CVC team has continued to move the project’s construction forward, and the Architect of the Capitol (AOC) is still proposing the same opening dates −− April 2007 for the base CVC project and May 2007 for the House and Senate expansion spaces −− but the Government Accountability Office (GAO) continues to believe that the proposed opening dates do not allow enough time to complete several critical activities and to address problems, challenges, risks, and uncertainties. As GAO reported, GAO estimates that the total cost to complete the entire CVC project is about $556 million without an allowance for risks and uncertainties and $584 million with such an allowance. To date, about $530 million has been provided for CVC construction. GAO estimates that the (AOC) will need about $25.6 million more in CVC construction funds to complete the entire CVC project. GAO plans to monitor and report on these costs to the Subcommittee as soon as AOC has a firmer estimate.
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−665T

33. *April 14, Department of Homeland Security* — **Protected Critical Infrastructure Information Program anniversary.** February 2006 marked the two−year anniversary of the Protected Critical Infrastructure Information (PCII) Program. The PCII Program, part of the Department of Homeland Security (DHS), facilitates secure information sharing between the private sector and government about the crucial systems, networks and facilities that support the nation’s day−to−day operations. Private industry owns and controls 85 percent of the nation’s critical infrastructure, such as railroads, power lines, hospitals, farms, communications and financial networks. The PCII Program, which commenced operation on February 18, 2004,

was created under the Critical Infrastructure Information Act of 2002 to enable those with knowledge of critical infrastructure to voluntarily share sensitive information by protecting it from public release under the Freedom of Information Act, state and local open records laws, and use in civil litigation. In the past six months alone, private sector submissions of critical infrastructure information have quadrupled. The Program has established numerous partnerships with entities like DHS's Risk Management Division and state homeland security initiatives that will bolster a successful future.
For more information, contact the PCII Program Office at (202) 360−3023 or visit http://www.dhs.gov/pcii
Source: http://cipp.gmu.edu/archive/cip_report_4.10.pdf

[Return to top]

Emergency Services Sector

34. *April 27, National Public Radio* — **Houston drill tests agencies' preparedness.** A mock explosion, fire, and oil spill in the Houston Shipping Channel, a lifeline for the nation's busy energy industry, provided a test this week for federal, state and local agencies and their ability to work together in the event of a terrorist attack. More than 300 people from nearly two−dozen agencies participated in the exercise. Initially, officials weren't told whether the incident was an act of terrorism. The shipping channel was closed as a precaution. Many aspects of the emergency were planned for, including Coast Guard teams with assault rifles and bomb−sniffing dogs to secure a pier, and at a joint information center, officials fielded calls from television networks and other media outlets. Agencies participating in the drill also included the FBI, Customs and Border Patrol, the Port of Houston Authority, and local police.
Source: http://www.npr.org/templates/story/story.php?storyId=5365695

35. *April 27, Claremore Daily Progress (OK)* — **CodeRED to alert citizens of emergencies.** A new Web database will enable Claremore, OK's emergency officials to keep the public better informed with regards to emergencies. "CodeRED" is a Web−based system that will allow the Claremore Police Department to notify city residents by phone in cases of current or impending emergency or crisis. "The CodeRED system will aid us in keeping the public informed whenever an emergency situation arises," said Mickey Perry, Claremore Chief of Police. Primary uses for the CodeRED system include search and rescue, environmental and national disasters, man−made disasters, and public works, which Chief Perry expected would be the most common usage of the system in Claremore. "The CodeRED system can send emergency−related messages to 1,600 homes a minute −− up to 60,000 in an hour −− there's no way we could do that without CodeRED."
Source: http://www.claremoreprogress.com/archive/article25833

36. *April 26, Government Technology* — **Alameda County, California, first responders to be linked via new digital radio system.** First responders in Alameda County, CA, will soon be linked via a new emergency radio system. The new Alameda County digital radio network replaces an analog radio network, and will provide the East Bay Region with interoperable radio communications for any agency that elects to use it. It will remove blockages in emergency communications caused by incompatible technologies and overcrowded frequencies across the region that have plagued East Bay police and fire agencies.

Source: http://www.govtech.net/news/news.php?id=99307

37. *April 26, Government Computer News* — **Interoperable communications needs common language.** Police and other emergency response departments in the national capital region of Virginia, Maryland and Washington, DC, have standardized on common 800MHz communications systems. What remains to be done in establishing interoperable systems is the unglamorous job of getting everyone on the same page. "The technical piece for the most part has been repaired since 9/11," said Captain Eddie Reyes of the Alexandria, VA, Police Department. "Now we have to focus on the human piece of interoperability." Some standards are in place. The Federal Communications Commission has set aside national mutual−aid channels in all three of the major public safety radio bands, UHF, VHF and the 800MHz band. "Most agencies have not taken the time to preprogram those frequencies into their radios, because they don't know about them," Reyes said. "It would solve a huge part of the interoperability problem if we could do that."
Source: http://www.gcn.com/online/vol1_no1/40559−1.html

38. *April 25, Christian Science Monitor* — **Oregon emergency system helps deploy first responders.** There is a growing network of public−safety responders in Oregon who are using a new Web−based technology to respond to emergencies. Mark Hanson, security director for Oregon's largest shopping center says, "When something pops up on my computer, I know I can look at it very quickly and assess the situation and know where our people need to go −− what needs to happen." Called RAINS, for Regional Alliances for Infrastructure and Network Security, this public−private coalition takes a bottom−up approach to emergency−response communications −− an approach quite different from the more centralized federal system. Supporters say RAINS helps crucial, time−sensitive reports flow more efficiently, though still securely, to different public−safety agencies, which potentially produces quicker and more effective responses. And the information−sharing system is quickly gaining more supporters: A number of communities across the United States are considering using the network's technology platform as well. Despite praise from homeland security experts, RAINS still encounters institutional resistance because of the reluctance to share information and hook up the technology. For example, the Portland police department has not linked to the system.
Source: http://www.csmonitor.com/2006/0425/p02s02−ussc.html

[Return to top]

Information Technology and Telecommunications Sector

39. *April 27, BBC News (UK)* — **Warnings over USB memory sticks.** Smart phones, iPods and USB memory sticks are posing a real risk for businesses, warn security experts. Just over half of companies take no steps to secure data held on these devices, found a UK government−backed security survey. Figures from the Information Security Breaches Survey, which is backed by the Department of Trade and Industry, reveals how firms are struggling to control the growing use of USB flash memory sticks. Matt Fisher, spokesperson for Centennial Software, said USB sticks could also become an attack vector for viruses and other malicious programs largely because they are swapped between many different computers.
Both the executive summary and the full results of the Information Security Breaches Survey, April 2006, can be found at:

http://www.pwc.com/Extweb/pwcpublications.nsf/docid/F9843CD3
C8E0FB828025715A0058C63B
Source: http://news.bbc.co.uk/2/hi/technology/4946512.stm

40. *April 26, Security Focus* — **Cisco VPN 3000 Concentrator malformed HTTP/TCP packet remote denial−of−service vulnerability.** Cisco VPN 3000 Concentrator is prone to a remote denial−of−service vulnerability when handling specially crafted HTTP or TCP packets. Analysis: This remote exploit involves sending a small stream less than 50 packets of tcp/80 traffic to a Cisco VPN 3000 Concentrator appliance running the WebVPN service. After this occurs, all sessions currently accessing the appliance are dropped, and no further communication is possible until the system is powered down and restarted. No authentication or credentials are required to exercise this vulnerability. By default, the WebVPN Service permits both tcp/80 (HTTP) and tcp/443 (HTTPS) inbound; the appliance performs a redirect from the HTTP query to the HTTPS. The vulnerability exists within the code base responsible for the redirect.
For a complete list of vulnerability details: http://www.securityfocus.com/bid/16394/info
Solution: Cisco has released advisory cisco−sa−20060126−vpn to address this issue:
http://www.cisco.com/warp/public/707/cisco−sa−20060126−vpn.s html
Source: http://www.securityfocus.com/bid/16394/references

41. *April 26, Security Focus* — **Mozilla Firefox large history file buffer overflow vulnerability.** Mozilla Firefox is reportedly prone to a remote denial−of−service vulnerability. Analysis: The browser handles a large entry in the 'history.dat' file. An attacker may trigger this issue by enticing a user to visit a malicious Website and by supplying excessive data to be stored in the affected file. Note: Proof−of−concept exploit code has been published. The author of the code attributes the crash to a buffer−overflow condition. Symantec has not reproduced the alleged flaw.
For a complete list of vulnerable products: http://www.securityfocus.com/bid/15773/info
Solution: For more information: http://www.securityfocus.com/bid/15773/references
Source: http://www.securityfocus.com/bid/15773/discuss

42. *April 26, Associated Press* — **Data to be sent using different colors of light.** By sending data using different colors of light, operators of the ultrahigh−speed Internet2 network are hoping to boost capacity by as much as 80−fold to enable researchers to connect telescopes around the world and perform other bandwidth−intensive tasks. The new network should be in place by fall 2007, said Douglas Van Houweling, Internet2's chief executive. He announced the plans this week as researchers set a new networking speed record −− 8.8 gigabits per second. The Internet2 network, parallels the regular Internet to let universities, corporations and researchers share large amounts of information in real−time. More than 200 U.S. universities now belong to the non−profit Internet2 consortium.
Source: http://www.msnbc.msn.com/id/12502711/

43. *April 26, IDG News Service* — **Bugs put widely used DNS software at risk.** A number of flaws in the software that is used to administer the Internet's Domain Name System (DNS) have been discovered by researchers at Finland's University of Oulu. The vulnerabilities could be exploited to "cause a variety of outcomes," according to an advisory, posted Wednesday, April 26, by the UK's National Infrastructure Security Coordination Center. Oulu researchers have

created a DNS test suite that can be used to test for these vulnerabilities, and a number of DNS software providers, have confirmed that some of their products are vulnerable.
For more information, see the UK National Infrastructure Security Coordination Center site:
http://www.niscc.gov.uk/niscc/docs/re−20060425−00312.pdf?lan g=en
Source: http://www.computerworld.com/securitytopics/security/holes/story/0,10801,110897,00.html

44. *April 26, Associated Press* — **Survey: 73 percent of adults in U.S. use the Internet.** The U.S. online population has hit an all−time high: 73 percent of adults, or 147 million, now use the Internet. The figures represent an increase from 66 percent, or 133 million adults, in January 2005, according to the Pew Internet and American Life Project.
Survey: Internet Penetration and Impact April 2006:
http://www.pewinternet.org/pdfs/PIP_Internet_Impact.pdf
Source: http://abcnews.go.com/Technology/wireStory?id=1893981

45. *April 26, Government Technology* — **Trust in online transactions to be measured.** The International Telecommunication Union is conducting a worldwide public survey to assess users' trust of online transactions and awareness of cybersecurity measures. The data collected through the survey will be used to increase global awareness of cybersecurity, particularly in developing countries, and should help decision−makers in assessing the cyberspace "trust" level with a view to reviewing national and corporate strategies and priorities.
Survey: http://www.itu.int/newsroom/wtd/2006/survey/index.html
Source: http://www.govtech.net/magazine/story.php?id=99322

46. *April 26, CNET News* — **Widespread AT&T DSL outage reported.** AT&T confirmed that hundreds or even thousands of customers in at least three states −− Ohio, Michigan, and Illinois −− suffered from a widespread DSL outage on Wednesday, April 26. A company spokesperson said the outage was due to a software upgrade on DSL equipment serving the customers in these regions.
Source: http://news.com.com/2061−10785_3−6065475.html?part=rss&tag=6065475&subj=news

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of publicly available exploit code and materials explaining how to exploit a race condition vulnerability in Sendmail. Sendmail improperly handles asynchronous signals causing a race condition vulnerability. Successful exploitation may allow a remote, unauthenticated attacker to execute arbitrary commands with the privileges of the user. For more information please review the following:

TA06−081A − Sendmail Race Condition Vulnerability
http://www.us−cert.gov/cas/techalerts/TA06−081A.html

VU#834865 − Sendmail contains a race condition
http://www.kb.cert.org/vuls/id/834865

Sendmail MTA Security Vulnerability Advisory
http://www.sendmail.com/company/advisory/

US−CERT recommends the following actions to mitigate the security risks:

Upgrade to the latest version: Sendmail 8.13.6.
http://www.sendmail.org/releases/8.13.6.html

Review the Sendmail MTA Security Vulnerability Advisory for steps to reduce the impact of this vulnerability. http://www.sendmail.com/company/advisory/#mitigation

US−CERT is not aware of any working exploit code at this time.

Phishing Scams
US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT.
http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 50497 (−−−), 445 (microsoft−ds), 6881 (bittorrent), 4343 (unicall), 55620 (−−−), 135 (epmap), 139 (netbios−ssn), 80 (www), 1025 (win−rpc) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

47. *April 27, Associated Press* — **Construction begins at Ground Zero.** Politicians and developers on Thursday, April 27, celebrated the start of construction on the Freedom Tower, a 1,776−foot−high skyscraper designed to replace the World Trade Center. On Wednesday, April

26, the Port Authority of New York and New Jersey, which owns the property, approved a broad deal with developer Larry Silverstein to move the project forward. Under that agreement, five towers will rise from the 16−acre site by 2012, joining a memorial and transit hub scheduled to open in 2009, and a performing arts center. For the next month, crews will be relocating utilities and making other preparations for laying the building's foundation. New York Governor George Pataki addressed concerns about the tower being a potential terrorist target while at the site with New Jersey Governor Jon Corzine, Mayor Michael Bloomberg, and Silverstein. The Freedom Tower so far has no tenants committed, although the Port Authority said nearly half of it would be filled with government leases. The tower was redesigned after police expressed concerns that the building was not sturdy enough to withstand a terrorist's truck bomb.
Source: http://abcnews.go.com/US/wireStory?id=1897099

[Return to top]

General Sector

Nothing to report.

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non−commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.